IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant(s): | Messaoud Benantar | | |
| Assignee: | International Business Machines Corporation | | |
| Title: | Method and System for Computing Digital Certificate Trust Paths Using Transitive Closures | | |
| Serial No.: | 10/045,112 | Filing Date: | January 10, 2002 |
| Examiner: | Shin Hon Chen | Group Art Unit: | 2431 |
| Docket No.: | AUS920010943US1 | Customer No. | 65362 |

May 20, 2009

*Filed Electronically*

**REPLY BRIEF UNDER 37 CFR § 41.41**

Dear Sir:

Applicant submits this Reply Brief in response to the Examiner's Answer mailed in this case on March 20, 2009. This reply will address selected arguments from the Examiner in the "Response to Argument" section of the Examiner's Answer, but will not attempt to address every argument since Applicant's Appeal Brief has previously addressed the appeal issues. It is believed that no fees are due in connection with the filing of this Reply Brief, however, the Commissioner is authorized to deduct any amounts required for this Reply Brief and to credit any amounts overpaid to Deposit Account No. 090447.

Regarding the anticipation rejection of the pending claims 1-9, 24, 27, and 30, Applicant respectfully submits that the separately recited claim requirements of "performing a transitive closure computation" and "performing an all-pairs-shortest-paths computation" on the adjacency matrix has not been disclosed or suggested by the prior art. In particular, the Examiner relies on Van Oorschot's description of the compilation of certificate chain data to generate a table of trust relationships (at column 4, lines 52-62, col. 10, lines 59-62, and the "intermediate level certificate chain data 209" in Figure 7a) to meet the claim requirement of "performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities." Examiner's Answer, p. 7. The Examiner then asserts that Van Oorschot's compilation of certificate chain data is "different from the shortest-path computation (VO: column 4 lines 65-67

and figure 7b; column 11 lines 24-26: the shortest path table is the **high level** certificate chain data) in which the compilation of certificate chain data takes place before the shortest-path computation to ensure validity of path." Id. With all due respect, the cited Van Oorschot description of compiling certificate chain data in no way discloses or suggests "performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities." There is no reference anywhere in Van Oorscot to an "adjacency matrix," much less to any separate step of performing a "transitive closure computation on the adjacency matrix." Indeed, when the *entirety* of the cited Van Oorschot passage is considered, it becomes apparent that the "shortest trusted path" is an example of what is generated when Van Oorschot's certificate chain data is compiled, so there is no separate "transitive closure computation" disclosed by Van Oorschot:

> For example, **where a high degree of compilation is performed**, the certificate chain data may be a list of all certification authorities in a **shortest trusted path** starting with a subscriber's own CA and ending with the target CA that issued the certificate of the subscriber that sent a digitally signed message. The compiled certification authority trust data serves as certificate chain data that may be for example, a table of trust relationships among the certificate issuing units in a community of interest, to facilitate rapid validity determination of the certificate by a plurality of requesting units. By way of example, **the compilation may consist of populating a database** that can be repeatedly queried by multiple subscribers to provide a preferred chain of certificates in a **shortest trusted path** among two subscribers, or between their respective CAs. If preferred, the stored certificate chain data can also include the associated certificates, or other information such as revocation status information related to the associated certificates, for each of the certificate issuing units listed in the table.

Van Oorschot, col. 4, lines 52-67 (emphasis added). As the passage shows, the referenced compilation of certificate chain data from Van Oorschot is not separate from the "all-pairs-shortest-paths" computation, and therefore does not anticipate the separately claimed requirement of "performing a transitive closure computation." However, as seen in claim 1's separate recitation of the "transitive closure" and "all-pairs-shortest-path" computations, the recited "transitive closure computation" is distinct from the "all-pairs-short-path" computation, and is used to immediately determine whether a trust path exists between two certificate authorities before the actual path is determined. Applicant submits further that those skilled in the art would understand that the transitive closure algorithm differs from the shortest path algorithm in that Van Oorschot requires storing the pairs of shortest paths, while the transitive

closure calculations are simpler since they only deal with a true or false answer (where true means there is a path between two nodes and false otherwise) so that the transitive closure only needs to store the boolean true or false for each given pair of CA certificates (0, or 1) that can be minimized to the bit-wise level. Because of at least these differences between Van Oorschot and claims 1-9, 24, 27, and 30, Applicant requests that the anticipation rejection of claims 1-9, 24, 27, and 30 be withdrawn and that the claims be allowed.

Regarding the anticipation rejection of pending claims 10-30, Applicant respectfully submits that the claim requirement of having a certificate authority send "a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web" has not been disclosed or suggested by the prior art. In particular, the Examiner relies on Van Oorschot's description of the certificate chain data 209 being "periodically updated" (at column 5, lines 53-60 and Figure 3) to meet the claim requirement of "sending a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web." Examiner's Answer, p. 8. While this passage refers to periodic updating of the certificate chain data 209, **there is absolutely no indication from the cited Van Oorschot passage of having a certificate authority send a "trust relation update message" to a central trust web agent, much less using the received "trust relation update message" to modify the set of trust relations at the central trust web agent.** Indeed, Van Oorschot discloses the reverse process for updating the certificate chain database 208 by having the certificate chain data generator 400 **periodically poll** the distributed directory 302 or other sources of certificate data to determine whether updates in the certificate trust data have occurred. Van Oorschot, col. 7, line 62 to col. 8, line 13. Thus, Van Oorschot fails to disclose or suggest having the certificate authorities send a trust relation update message to a central trust web agent to modify the set of trust relations for the certificate authorities as variously recited in claims 10-30. Because there is no disclosure or suggestion by Van Oorschot of sending a "trust relation update message" to a central trust web agent which "processes trust relation information for a set of certificate authorities within a trust web," Applicant submits that a *prima facie* showing of anticipation has not been established. Similarly, there has been no *prima facie* showing that Van Oorschot discloses the requirement of "modifying a set of trust relations for the set of certificate authorities within the trust web based on an indicated request in the trust

relation update message" as variously recited in claims 22-30. Because of at least these differences between Van Oorschot and claims 10-30, Applicant requests that the anticipation rejection of claims 10-30 be withdrawn and the claims be allowed.

## CONCLUSION

A *prima facie* case of anticipation has not been established because the cited art fails to disclose Applicant's claimed scheme for computing digital certificate trust paths by "performing a transitive closure computation on the adjacency matrix …" that is separate and apart from the step of "performing an all-pairs-shortest-paths computation," as variously recited in claims 1-9, 24, 27, and 30. Nor does the cited art disclose Applicant's scheme for having a certificate authority send "a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web," as variously recited in claims 10-30. Accordingly, it is respectfully urged that the rejection of the claims should not be sustained.

CERTIFICATE OF TRANSMISSION

I hereby certify that on May 20, 2009, this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

*/Michael Rocco Cannatti/*

Respectfully submitted,

*/Michael Rocco Cannatti/*

Michael Rocco Cannatti
Attorney for Applicant(s)
Reg. No. 34,791